

Zero Trust-Netzwerkzugang

Die Zero Trust-Dienste von Cloudflare, insbesondere Access, steigern die Teamproduktivität und verringern das Risiko, weil alle Nutzer ohne VPN auf Ihre Anwendungen zugreifen können – ob selbstgehostet, als SaaS bereitgestellt oder offline.

Unkomplizierter und sicherer Zugriff für hybrides Arbeiten

Internetnativer Zero Trust Network Access (ZTNA)

Die heutige dezentrale Arbeitsumgebung erfordert einen dezentralen Sicherheitsansatz. Der „Sicherheitsperimeter" existiert nicht mehr und herkömmliche Fernzugriffslösungen wie VPNs können die modernen Erwartungen an Sicherheit und Performance nicht erfüllen.

ZTNA überprüft für jede einzelne Ressource kontinuierlich den genauen Kontext, also etwa Identität und Gerätestatus. Das ermöglicht jedem Nutzer einen unkomplizierten, sicheren, geräte- und ortsunabhängigen Zugriff auf alle Anwendungen. Dank dieses völlig neuen Ansatzes muss nicht mehr zwischen Sicherheit und Nutzererfahrung abgewogen werden: ZTNA unterstützt Ihr Unternehmen durch die Verbesserung beider Aspekte.

Die Anwendung dieses Konzepts macht Unternehmen auch flexibler und erleichtert es ihnen, Veränderungen zu bewältigen – sei es bei der Cloud-Migration, bei Fusionen und Übernahmen oder bei Innovationen und schneller Skalierung. Cloudflare bildet das Herzstück einer Zero Trust- oder Sicherheitsmodernisierungsstrategie und ermöglicht ZTNA über eine programmierbare, globale Connectivity Cloud.

80% durchschnittliche Zeitersparnis bei der Bearbeitung von IT-Tickets im Zusammenhang mit der Verwendung eines VPN beim Fernzugriff-Support[1]

72% Zeitersparnis bei monatlicher Richtlinienkonfiguration im Vergleich zum vorherigen Anbieter[1]

68% sahen erheblichen Beitrag zur Optimierung der Authentifizierungsverfahren für Mitarbeitende und Auftragnehmer[1]

Modernere Zugriffsmethoden verschaffen Ihrem Unternehmen mehr Bewegungsfreiheit



Nutzererfahrung verbessern

Steigern Sie die Teamproduktivität mit modernisierter Sicherheit, die dafür sorgt, dass sich lokale Anwendungen genauso anfühlen wie SaaS-Applikationen: Keine langsamen, schwerfälligen VPNs mehr, keine Beschwerden von Angestellten.



Laterale Bewegung unterbinden

Reduzieren Sie Cyberrisiken und verkleinern Sie Ihre Angriffsfläche, indem Sie kontextbasierten Zugriff mit minimalen Zugriffsrechten pro Ressource statt Zugriff auf Netzwerkebene gewähren.



Zero Trust mühelos skalieren

Indem Sie zuerst kritische Anwendungen oder Nutzergruppen mit dem höchsten Risiko schützen und dann den internetnativen ZTNA erweitern, um Ihrem gesamten Unternehmen Schutz zu bieten, erhöhen Sie die technische Effizienz.

Häufige Anwendungsfälle für Access

Sicheres hybrides Arbeiten

-  **VPN-Ergänzung und -Ersatz** – Access ist schneller und sicherer als herkömmliche VPNs. Beginnen Sie mit der Auslagerung kritischer Anwendungen für mehr Sicherheit und ein besseres Nutzererlebnis.
-  **Zugang für Auftragnehmer** – Authentifizieren Sie Nutzer von Drittanbietern wie Auftragnehmer mit clientlosen Optionen, Social IdPs und mehr.
- **Zugang für Entwickler** – Ermöglichen Sie technischen Usern mit weitergehenden Rechten sicheren Zugriff auf kritische Infrastruktur, ohne die Performance zu beeinträchtigen.

Digitale Modernisierung

- **Beschleunigung von Fusionen und Übernahmen** – Vermeiden Sie eine herkömmliche Netzwerkverschmelzung vollständig. Integrieren Sie mehrere IdPs und legen Sie während Fusionen und Übernahmen die internen Zugriffsrechte für jede Anwendung einzeln fest.
- **Cloud-Migration** – Erhalten Sie die Geschäftskontinuität in Veränderungsphasen, z. B. bei der Migration von Anwendungen oder Identitätsverzeichnissen in die Cloud.
- **Phishing-resistente MFA** – Führen Sie starke Authentifizierung, wie FIDO2-konforme Security-Token, überall ein.

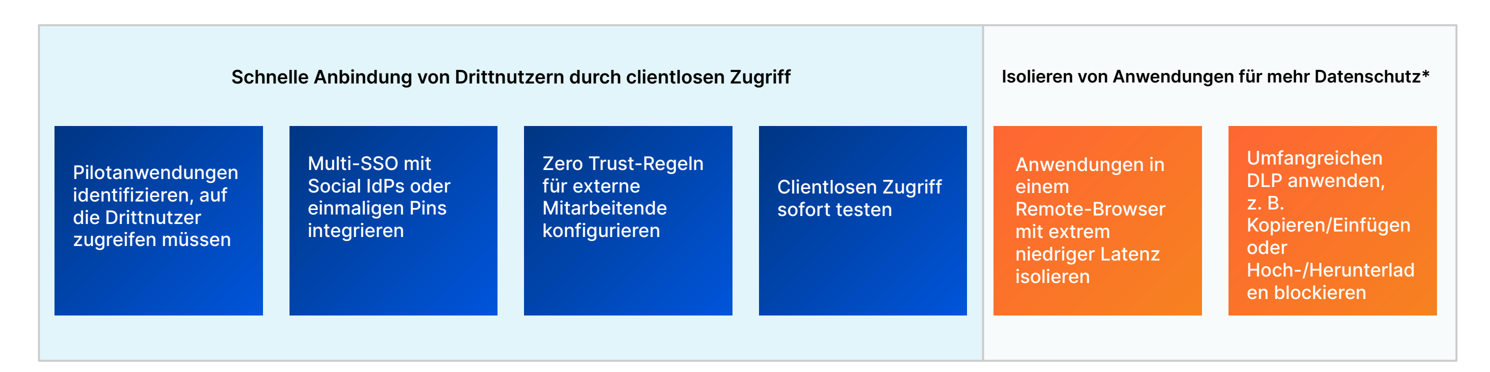
VPN-Ergänzung und -Ersatz: Erste Schritte

Geben Sie bei einer ZTNA-Piloteinführung kritischen Anwendungen oder risikobehaftete Nutzern Vorrang, um Ihr VPN zu ergänzen. Nutzen Sie den clientlosen Zugriff für Webanwendungen oder SSH im Browser, um das Testen zu beschleunigen. Führen Sie im Laufe der Zeit erweiterte Funktionen ein, um Ihr VPN vollständig zu ersetzen und eine dynamische Sichtbarkeit zu erhalten, wenn sich Ihr Netzwerk verändert.



Zugriff von Auftragnehmern: Erste Schritte

Sorgen Sie für eine reibungslose Nutzererfahrung und minimieren Sie gleichzeitig das Risiko, das von nicht verwalteten Geräten ausgeht. Konfigurieren Sie einfache Authentifizierungsoptionen für Auftragnehmer – Software für Endnutzer ist nicht erforderlich. Führen Sie im Lauf der Zeit erweiterte Funktionen ein, um den Datenschutz weiter zu verbessern.



Nutzung von Funktionen in anderen Teilen der Zero Trust-Plattform

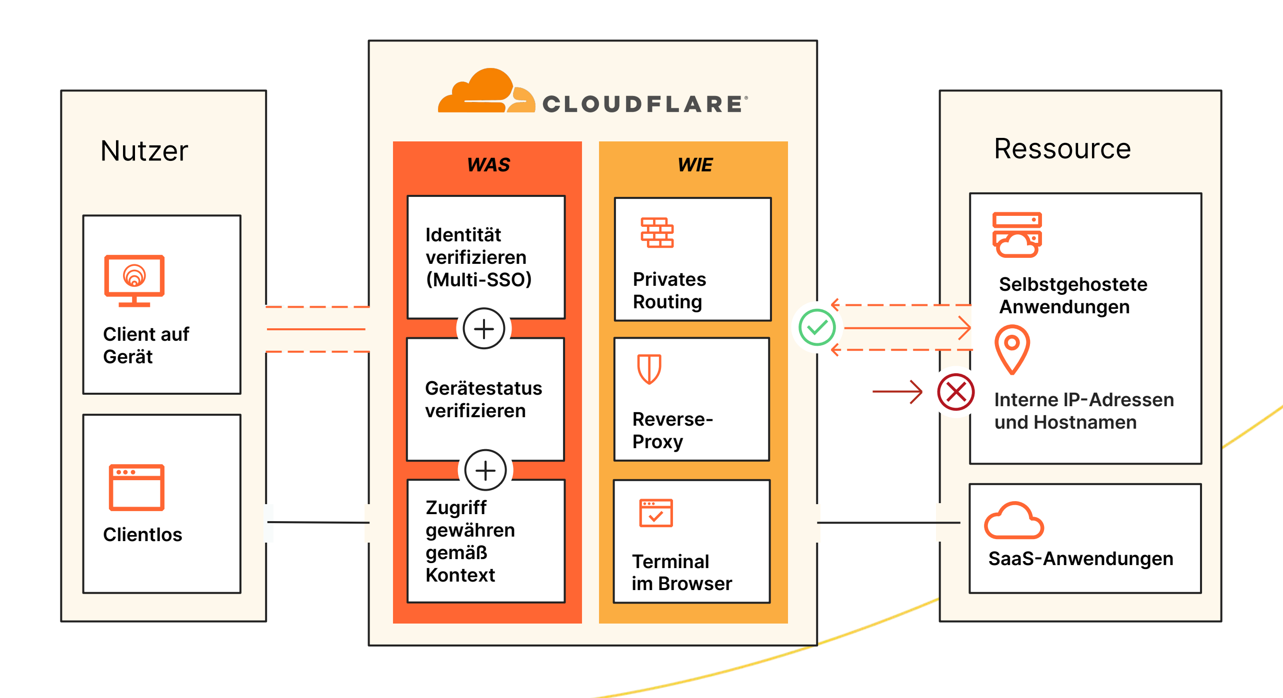
Funktionsweise von Access

Cloudflare Access ist eine flexible Aggregationsschicht, die kontinuierlich granulare Kontexte wie Identität und Gerätestatus überprüft, um einen einfachen, sicheren Zugang zu allen Ressourcen eines Unternehmens zu ermöglichen und einen softwaredefinierten Sicherheitsperimeter zu schaffen. Wenn sich ein Nutzer authentifiziert und alle Kriterien der Zugriffsrichtlinien erfüllt, stellt Access ein signiertes JSON-Web-Token aus, das für eine bestimmte Sitzungsdauer gültig ist. Wir führen eine Single-Pass-Überprüfung aller Nutzeranfragen über unsere modulare Plattform durch und unsere zentrale Richtlinienverwaltung ermöglicht dank unserer einzigartigen Anycast-Netzwerkarchitektur globale Richtlinienänderungen innerhalb von Sekunden.

Einheitlicher clientloser und clientbasierter Betrieb für alle Gerätetypen. Wir verwenden einen einzigen Geräte-Client für alle Zero Trust-Dienste. Dieser verschlüsselt den an unser Netzwerk gerichteten Traffic, um die Daten unserer Kunden zu schützen. Durch unsere clientlose Struktur bieten wir auch einfachen, sicheren Zugriff auf Geräte außerhalb des Unternehmens. Unsere ZTNA- und DNS-Services sowie unsere marktführenden WAF- und DDoS-Schutzdienste arbeiten zusammen, um öffentliche Hostnamen zu erstellen und abzusichern, auf die Nutzer von Drittanbietern und hybrid arbeitende Beschäftigte von jedem Gerät aus zugreifen können. Unsere Optionen zur nutzerlosen Authentifizierung (Token oder mTLS-Zertifikate) sind auch für automatisierte Dienste und IoT-Geräte geeignet.

Für Zero Trust-Kontrollen verwenden Ressourcen öffentliche Hostnamen zum Einsatz eines Reverse-Proxy in Richtung selbstgehosteter (cloudbasierter/lokaler) Anwendungen oder SSH/VNC im Browser, zum Einsatz eines Identitäts-Proxy in Richtung von SaaS-Anwendungen oder Client-/Tunnel-basiertes privates Routing über einen L4-7-Forward-Proxy in Richtung jeder Web- oder Nicht-Web-Ressource (z. B. beliebige TCP/UDP) innerhalb eines privaten Subnetzes. Anders als andere Zero Trust-Anbieter unterstützt unsere globale Netzwerk- und Anwendungs-Konnektor-Software in Kombination jede Rechenumgebung – ob Public Cloud, einschließlich Kubernetes und Container, oder herkömmliche lokale Netzwerkressourcen – ohne VM-Infrastruktur und ohne Durchsatzbeschränkungen.

Identitäts-, Endpunkt-, Netzwerk-On-Ramping-, Protokollierungs-/Analyse- und SIEM-Tools von Drittanbietern sind neben nativen Optionen für unseren Geräte-Client und Analysen in unser Dashboard integriert, sodass Administratoren agil bleiben und mit den ihnen bereits vertrauten Tools arbeiten können.



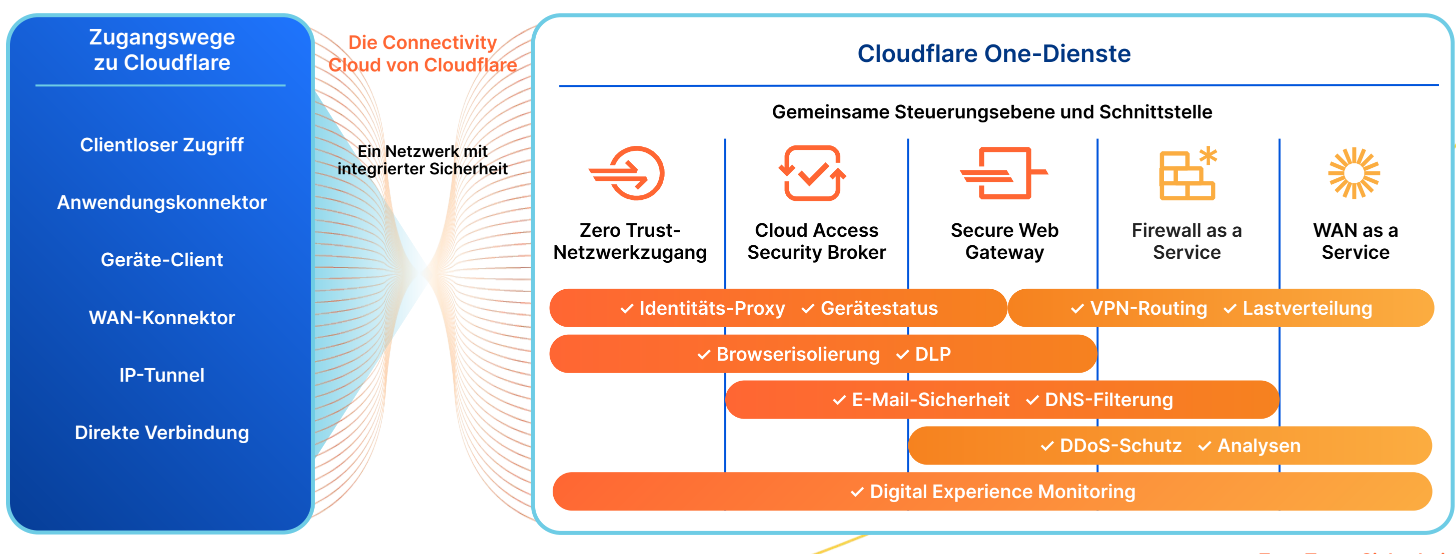
Access als Teil der SSE- und SASE-Plattform von Cloudflare

SSE und SASE bedeuten oft eine mehrjährige strategische Entwicklung. Bei Cloudflare beobachten wir häufig, dass Unternehmen mit ZTNA beginnen, da dieses Konzept für IT-Teams umsetzbare und leicht zugängliche Schritte beinhaltet und gleichzeitig einen erheblichen kurzfristigen geschäftlichen Nutzen bietet. IT-Führungskräfte wollen auf ihrem Weg zur Konsolidierung hybride Arbeit absichern, Bedrohungen abwehren und ihre Daten schützen. Dafür entscheiden sie sich zunehmend für Cloudflare als vertrauenswürdigen Partner.

Die flexible Implementierung und modulare Architektur von Cloudflare ermöglichen es jedem Unternehmen, die Performance von Geräten, Anwendungen und ganzen Netzwerken zu steigern und diese zu schützen. So können sie dafür sorgen, dass hybride Arbeiten sicher und produktiv bleibt. Dazu unterstützen wir das agentenlose Onboarding für Endnutzer, die clientlose Webisolierung zur Eindämmung von unsicherem Datenverkehr und ein gemeinsames Verwaltungs-Dashboard, das Einblick in alle Sicherheits- und Netzwerkdienste gewährt – und zwar unabhängig davon, von wo aus sich Administratoren oder Nutzer verbinden. Dank der Reichweite des globalen Cloudflare-Netzwerks können Sicherheitsmaßnahmen in größerer Nähe zu den Endnutzern durchgesetzt, die Latenz minimiert und den Mitarbeitenden ein reibungsloses Arbeiten ermöglicht werden. Unsere Anycast-Architektur hilft bei der Umgehung von Internetstörungen, sodass Teams online bleiben und die Geschäftskontinuität gewährleistet ist.

Bei unserer konsolidierten SSE- und SASE-Plattform trägt der gemeinsame Kontext unserer ZTNA-, CASB-, DLP- und SWG-Richtlinien dazu bei, das Sicherheitsniveau zu verbessern und gleichzeitig die Implementierung durch einen einheitlichen Verwaltungs-Workflow zu vereinfachen. Dieselben Identitäts- und Geräteattribute können sowohl in die Zugriffsrichtlinien für ZTNA und CASB als auch in die SWG-Richtlinien einfließen, was die unternehmensübergreifende Richtlinienverwaltung erleichtert.

ZTNA, RBI und E-Mail-Sicherheit können auch zusammen eingesetzt werden, um den bedingten Zugriff auf Ressourcen zu ermöglichen und gleichzeitig die Nutzer vor schädlichen Inhalten (Links, Anhänge) zu schützen, denen sie über E-Mail- und Tools zur Zusammenarbeit ausgesetzt sind. Auftragnehmern und Anwendern auf nicht verwalteten Geräten kann begrenzter Zugriff auf Firmenressourcen gewährt werden, wobei Nutzerinteraktionen (z. B. Upload/Download, Kopieren/Einfügen, Tastatureingabe) deaktiviert werden, um Datenkompromittierung zu verhindern. Andere L7-DLP-Richtlinien können angewendet werden, um sensible Daten zu erkennen.



Das sagen unsere Kunden

„Cloudflare Access ist eine fantastische Alternative zu herkömmlichen VPNs. Die Nutzer öffnen einfach ihren Browser und melden sich an, ohne zusätzliche Software herunterladen und konfigurieren zu müssen."

— **Platzi**, Head of Cloud Engineering

„Wenn man den Zugang zu internen Ressourcen beschränken will, ist Access viel einfacher zu handhaben und sicherer als ein VPN. Wir aktivieren die Lösung nur und fügen Nutzer hinzu. Es funktioniert einfach!"

— **Bitpanda**, CTO und Mitgründer

„Cloudflare war genau zum richtigen Zeitpunkt verfügbar, sodass wir uns die Mühe sparen konnten, ein VPN einzusetzen. Die Entscheidung ist uns leichtgefallen und die Lösung war erschreckend einfach zu implementieren."

— **ezCater**, Head of Security

„Bevor wir Cloudflare implementiert haben, dauerte es zwei bis vier Wochen, eine Anwendung sicher bereitstellen zu können. Mit Cloudflare Zero Trust können wir diesen Zeitaufwand um fast 90 % reduzieren."

— **Creditas**, Network Engineering Team Lead

Das sagen Analysten



Cloudflare wird bei IDC MarketScape 2023 als Marktführer („Leader") für Zero Trust Network Access (ZTNA) eingestuft

IDC verweist auf die „aggressive Produktstrategie von Cloudflare zur Unterstützung der Sicherheitsanforderungen von Unternehmen". Wir glauben, dass diese Anerkennung unseren Ansatz bestätigt, Unternehmen jeder Größe den Einstieg in Zero Trust und den sicheren Zugang für jeden Nutzer zu jeder Ressource ohne VPNs zu ermöglichen.



Cloudflare wird im KuppingerCole Leadership Compass 2022 als Marktführer („Leader") im Bereich ZTNA genannt

Im Rahmen ihrer ZTNA-Marktanalyse 2022 nannte die KuppingerCole Analysts AG mehrere Stärken von Cloudflare, wie unsere vollständig integrierte, organisch entwickelte Sicherheitsplattform, unsere große globale Cloud-Infrastruktur und unsere massive Marktpräsenz.



Funktionen von Access

Erstellen/Bearbeiten von Zero Trust-Richtlinien für sicheren Zugriff	
Granulare, benutzerdefinierte Zugriffsrichtlinien	Zentrale Richtlinienverwaltung. L7-Anwendungen werden auf Subdomain- und Pfad-Ebene mit Wildcard- und Multi-Hostname-Unterstützung abgesichert und unterstützen CORS-Anfragen. Richtlinienänderungen werden binnen Sekunden weltweit umgesetzt. Ein Richtlinientester ist inbegriffen.
Breite Palette an Ressourcen: Was wir schützen können und wie	Ressourcen verwenden öffentliche Hostnamen zum Einsatz eines Reverse-Proxy in Richtung selbstgehosteter Anwendungen (cloudbasiert/lokal) oder SSH/VNC im Browser, zum Einsatz eines Identitäts-Proxy in Richtung SaaS-Anwendungen oder Client-/Tunnel-basiertes privates Routing per L4–7-Forward-Proxy* in Richtung jeder (beliebigen TCP-/-UDP)-Ressource (sowohl im Web als auch außerhalb) innerhalb eines privaten Subnetzes.
Identität	Authentifizierung über alle wichtigen Firmen- und Social-Identitätsanbieter (IdP), einschließlich mehrerer IdPs gleichzeitig. Auch generische SAML- und OIDC-Konnektoren können genutzt werden. Unterstützung (und gegebenenfalls Durchsetzung) jeder von IdPs angebotenen AuthN-Methode, temporäre AuthN, Zweckrechtfertigung, Re-AuthN-Intervalle auf globaler oder Anwendungs-Sitzungsbasis und sofortige Sitzungswiderrufsoption pro Anwendung oder pro Nutzer.
Gerätestatus	Der Gerätestatus wird mithilfe von Geräteclients und EPP (Endpoint Protection Provider)-Integrationen von Drittanbietern überprüft. Mit Service-to-Service-Integrationen können EPP-Risikobewertungen in Zero Trust-Richtlinien einbezogen werden.
Kontextbezogene Signale für Richtlinien	Signale wie E-Mail-Gruppen, IP-Bereiche, Geolocation, Anmeldemethoden (z. B. MFA-Typ, IdP-Typ), gültige mTLS- oder SSH-Zertifikate, Service-Token, Seriennummernlisten, Gerätezustandsattribute, installierte Geräteclients, Sitzungsdauer, SWG-Regeldurchsetzung oder Signale von externen API-Aufrufen können konfiguriert werden. Auch ein Direktverweis auf Microsoft Entra ID (Azure AD)-Richtlinien für bedingten Zugriff ist möglich.
Weitere verwandte Unterstützungen	• **SCIM:** Automatische Bereitstellung/Deprovisionierung von Nutzern für selbstgehostete Applikationen und SaaS-Anwendungen (Beispiele für Okta und Azure AD) • **Internes DNS:** Konfiguration eines lokalen Domain-Fallbacks und Auflösung von Anfragen an private Netzwerke • **Aufgeteilte Tunnel:** Ein- und Ausschließen von IP-Adressen für private Netzwerke oder Parallelbetrieb zu einem VPN • **mTLS-Authentifizierung:** Zertifikatsbasierte Authentifizierung für IoT und andere mTLS-Anwendungsfälle • **Anwendungsisolierung:** Mit einem einzigen Kontrollkästchen kann die Anwendungsisolierung in unserem blitzschnellen Remote-Browser* vorgenommen werden
On- und Offramping	
Anwendungsanschluss	Einfache Orchestrierung unseres leichtgewichtigen Anwendungskonnektors (Cloudflare Tunnel) beschleunigt die Verbindung von Ressourcen mit Cloudflare, ohne dass eine VM-Infrastruktur erforderlich ist und ohne Durchsatzbeschränkungen. Beinhaltet Überwachung, virtuelle Netzwerke (für IP-Adressen-Überschneidungen) sowie Redundanz- und Failover-Funktionen.
Geräte-Client: Anwendungsfälle	• **Clientlos:** Erweiterung der Zero Trust-Richtlinien auf Nutzer von Drittanbietern auf nicht verwalteten Geräten; auch gut mit clientloser RBI und L7-DLP-Richtlinien kombinierbar*. Der clientlose Zugriff unterstützt Webanwendungen und SSH/VNC im Browser. • **Clientbasiert:** Unser Geräte-Client (Cloudflare WARP) erweitert den sicheren Zugriff auf private Netzwerke, ermöglicht die Integration von Service-to-Service-Geräten und ist standortabhängig, um maßgeschneiderte Richtlinien für lokale Nutzer anzuwenden. Außerdem können zwei oder mehr Geräte, auf denen WARP läuft, miteinander verbunden werden, um private Netzwerke zu erstellen. Nutzer können sich selbst anmelden, es ist aber auch eine Bereitstellung per MDM möglich.
Erweiterbarkeit und Sichtbarkeit	
Seitenanpassung	Hochladen von benutzerdefiniertem HTML-Code für Blockier- und Anwendungsstartseiten, um diese an Ihr Branding anzupassen oder Übermittlung spezifischer Zugriffsanweisungen für eine optimierte der Nutzererfahrung.
Protokollierung	Umfassende Protokollierung für alle Anfragen, Nutzer und Geräte. Kann über Logpush oder API in vorhandene SIEM-, Orchestrierungs- und Analysetools integriert werden. Bei unbekannten Assets katalogisiert unser Schatten-IT-Dienst für interne Infrastruktur passiv den einzigartigen Datenverkehr, der alle Ursprungsserver zutage befördert.
Automatisierung	Intuitive APIs und Terraform-Anbieter sind verfügbar, um alle Aspekte einer Zero Trust-Implementierung programmatisch zu verwalten. Außerdem bieten wir nutzerlose Service-Token-Unterstützung für automatisierte Dienste.

**Nutzung von Funktionen in anderen Teilen der Zero Trust-Plattform*

Was spricht für Cloudflare?



Einfache Einrichtung und Verwaltung

Vereinfachen Sie das Setup und den Betrieb von eingehendem Traffic auf private Ressourcen mit Anwendungskonnektor-Software und Tunnel-Orchestrierung erheblich.



Reibungsloses, unterbrechungsfreies Erlebnis

Erzielen Sie mit der globalen Anycast-Technologie von Cloudflare eine Spitzenperformance für Endnutzer und profitieren Sie von unserer Ausfallsicherheit, um Zuverlässigkeit zu gewährleisten.



Schnelle, frühzeitige Innovationen

Halten Sie mit der Entwicklung des Internets selbst Schritt – mit einem Anbieter, der seine Konkurrenten ständig übertrifft, um einen schnelleren und sichereren Anwendungszugriff zu ermöglichen.

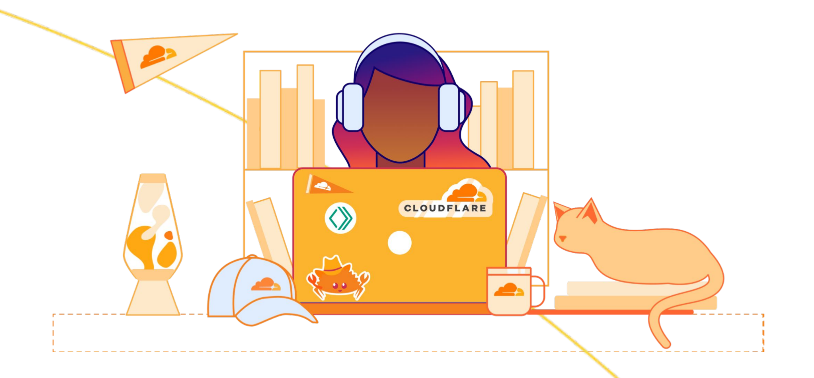
Lassen Sie uns über eine unkomplizierte und sichere Zugriffsrechteverwaltung für Ihr Unternehmen sprechen

Workshop-Termin vereinbaren



Noch nicht bereit für ein persönliches Gespräch?

Verschaffen Sie sich weitere Informationen zu der SSE- und SASE-Plattform von Cloudflare



1. Umfrage aus dem Jahr 2023: techvalidate.com/product-research/cloudflare/charts